JC927 U.S. PTO
09/29/00

10-02-00

A

Patent
Attorney's Docket No. 026125-069

JC929 U.S. PTO
09/676186
09/29/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

UTILITY PATENT
APPLICATION TRANSMITTAL LETTER

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Enclosed for filing is the utility patent application of Johan KIESSLING and Jan ARWALD for Method and Apparatus for Executing Secure Data Transfer in a Wireless Network.

Also enclosed are:

[X] 4 sheet(s) of [X] formal [ ] informal drawing(s);

[X] a claim for foreign priority under 35 U.S.C. §§ 119 and/or 365 [X] is hereby made to 9903560-2 filed in Sweden on October 1, 1999; [X] in the declaration;

[X] An unexecuted declaration of the inventor(s) also is enclosed.

[X] Please amend the specification by inserting before the first line the sentence --This application claims priority under 35 U.S.C. §§ 119 and/or 365 to 9903560-2 filed in Sweden on October 1, 1999; the entire content of which is hereby incorporated by reference.--

The filing fee has been calculated as follows [X] and in accordance with the enclosed preliminary amendment:

CLAIMS					
	NO. OF CLAIMS		EXTRA CLAIMS	RATE	FEE
Basic Application Fee				(101)	$ 690.00
Total Claims	20	MINUS 20 =	0	x $18 = (103)	0.00
Independent Claims	5	MINUS 3 =	2	x $78 = (102)	156.00
If multiple dependent claims are presented, add $260.00 (104)					0.00
Total Application Fee					846.00
If verified statement claiming small entity status is enclosed, subtract 50% of Total Application Fee					0.00
Add Assignment Recording Fee of $40.00 (581) if Assignment document is enclosed					0.00
TOTAL APPLICATION FEE DUE					**$846.00**

21839

[ ] This application is being filed without a filing fee. Issuance of a Notice to File Missing Parts of Application is respectfully requested.

[ ] A check in the amount of $_____ is enclosed for the fee due.

[X] Charge $ 846.00 _____ to Deposit Account No. 02-4800 for the fee due.

[X] The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800. This paper is submitted in duplicate.

Please address all correspondence concerning the present application to:
Ronald L. Grudziecki, Esquire
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

P.O. Box 1404
Alexandria, Virginia 22313-1404
(919) 941-9240

By: Michael G. Savage
Michael G. Savage
Registration No. 32,596

Date: September 29, 2000

"Express Mail" mailing label No. EL581399774US
Date of Deposit 9/29/00
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C 20231
H. Rattelade
(Type or printed name of person mailing paper or fee)
H. Rattelade
(Signature of person mailing paper or fee)

Patent
Attorney's Docket No. 026125-069

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Johan KIESSLING et al.	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: September 29, 2000	)	
	)	
For: Method and Apparatus for Executing Secure Data Transfer in a Wireless Network	)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Before examination, please amend this application as follows.

IN THE SPECIFICATION

Page 1, line 8, change "Field of the Invention" to --Background--; and

line 20, delete "Description of the Prior Art".

Page 3, line 16, delete "of the Invention".

Page 5, line 21, delete "of the Invention".

IN THE CLAIMS

Page 11, line 1, change "CLAIMS" to --What Is Claimed Is:--.

Claim 1, page 11, line 3, delete "(1)";

line 4, delete "(5)";

line 5, delete "(2, 3)" and (5);

line 6, delete "(1)" and "(301, 302; 401, 402)";

line 7, change "**characterised by**" to --comprising:--;

line 9, delete "(5)" and "(6)";

line 10, delete "(2, 3)" and "(303, 304, 305, 306; 403, 404)";

line 12, delete "(6)" and "(1)";
line 14, delete "(307, 308, 309, 310; 405, 406, 407, 408)";
line 16, delete "(311, 312; 409, 410)";
line 18, delete "(1)", "(6)", and "(313; 411)";
line 19, delete "(314; 412)"; and
line 21, delete "(315; 413)".

Claim 2, page 11, line 23, delete "characterised in"; and
line 24, delete "that" and insert therefor --wherein--, and delete "(5)"
line25, delete "(5)"
line 26, delete "(1)"
line 27, delete "(2, 3)" and "(5)"; and
line 28, delete "(1) (301, 402; 401, 402)".

Claim 3, page 11, line 30, delete "or 2, characterised by" and insert therefor --, comprising--;
line 34, delete "(1)";
line 35, delete "(5) (303; 403); and
line 26, delete "(5)" and "(1)".

Claim 4, page 12, line 1, delete "any of the preceding claims" and insert therefore -- claim 1--; and
line 3, delete "characterised in that" and insert therefor --wherein--;
line 4, delete "(6)" and "(1)";
line 8, delete "(308; 406)"
line 10, delete "(6)" and "(1)";
line 11, delete "(309; 407)";
line 13, delete "(1)"; and
line 14, delete "(310; 408)"

Claim 5, page 12, line 16, delete "any of the preceding claims" and insert therefore -- claim 1--; and

line 17, delete "characterised in that" and insert therefor --wherein--.

line 19, delete "(311; 409)"; and

line 21, delete "(312, 410)".

Claim 6, page 12, line 13, delete "any of the preceding claims" and insert therefore --claim 1--; and

line 24, delete "characterised in that" and insert therefor --wherein--;

line 27, delete "(5)" and "(1)";

line 28, delete "(304)" and "(305)"; and

line 29, delete "(6) (306)".

Claim 7, page 12, line 31, delete "any of the claims 4-6, char-" and insert therefor --claim 4,--; and

line 32, delete "acterised in that" and insert therefor --wherein--.

Claim 8, page 13, line 4, delete "characterised in"; and

line 5, delete "that" and insert therefor --wherein--; and

line 7, delete "(307; 405)".

Claim 9, page 13, line 10, delete "(1)"

line 11, delete "characterised by" and insert therefor --comprising-- and delete "(5)" and "(2, 3)";

line 12, delete "(6)" and "(2, 3)";

line 14, delete "(1)" and "(5)";

line 15, delete "(5)";

line 17, delete "(6)";

line 18, delete "(6)";

line 20, delete "(5)";

line 21, delete "(1)";

line 22, delete "(1)";

line 23, delete "(6)";

line 24, delete "(6)"; and

line 26, delete "(5)".

Claim 10, page 13, line 29, delete "characterised in"; and

line 30, delete "that" and insert therefor --wherein-- and delete "(1)".

Claim 11, page 14, line 1, delete "characterised in"; and

line 2, delete "that" and insert therefor --wherein--.

Claim 12, page 14, line 9, delete "any of the claims 9-11" and insert therefor --claim 9--; and

line 10, delete "characterised in that" and insert therefor --wherein--.

line 11, delete "(2)";

line 12, delete "(1)" and "(3)";

line 13, delete "(5)" and "(4)"; and

line 14, delete "(2)" and "(3)".

Claim 13, page 14, line 16, delete "characterised in"; and

line 17, delete "that" and insert therefor --wherein-- and delete "(6)"; and

line 18, delete "(4)".

Claim 14, page 14, line 20, delete "any of the claims 9-12" and insert therefor --claim 9--; and

line 21, delete "characterised in that" and insert therefor --wherein-- and delete "(6)"; and

line 22, delete "(5)".

Claim 15, page 14, line 24, delete "any of the claims 9-14" and insert therefor --claim 9--; and

line 25, delete "characterised in that" and insert therefor --wherein--; and

line 26, delete "(1)".

Claim 16, page 14, line 29, delete "characterised in"; and

line 30, delete "that" and insert therefor --wherein--.

Claim 17, page 15, line 2, delete "(2, 3)";
line 3, delete "(1)" and "(5)"; and
line 4, delete "characterised by" and insert therefor --comprising--.

Claim 18, page 15, line 18, delete "characterised by" and insert therefor --comprising--;
line 17, delete "(6)";
line 21, delete "(1)";
line 23, delete "(1)";
line 25, delete "(1)"; and
line 27, delete "(5)".

Claim 19, page 15, line 30, delete "(6)";
line 33, delete "(1)"; and
line 35, delete "(1)".
page 16, line 2, delete "(1)"; and
line 4, delete "(5)".

"Express Mail" mailing label No. EL581399774US
Date of Deposit 9/29/00
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231
H. Rattelade
(Type or printed name of person mailing paper or fee)
(Signature of person mailing paper or fee)

REMARKS

The written description and claims have been amended and the Abstract has been replaced to place the application in better form for examination. Favorable consideration is respectfully solicited.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: Michael G. Savage
Michael G. Savage
Registration No. 32,596

P.O. Box 1404
Alexandria, Virginia 22313-1404
(919) 941-9240

Dated: September 29, 2000

ABSTRACT

A method for executing secure data transfer between a communication device and an application server in a wireless network, in which a request requiring a secure transaction of data is sent from either the communication device or the server. An agreement proposal for the secure transaction is sent to the communication device, and if the agreement proposal is considered acceptable, the agreement proposal is sent to a security adapter. Details of the transaction are entered into a message and sent to a smart card in order to activate a signing application in the smart card. The details of the transaction are displayed on the communication device, and if the transaction is accepted, the signing application signs the data and sends it to the security adapter via messages, the signature is verified, and the data is sent to the server.

APPLICANT: TELEFONAKTIEBOLAGET L M ERICSSON (publ)

TITLE: METHOD AND APPARATUS FOR EXECUTING SECURE DATA TRANSFER IN A WIRELESS NETWORK

Field of the Invention

The present invention relates to a method and apparatus for secure data transfer between a communication device and an application server in a wireless network, and more particularly to a method for secure data transfer between a communication device, provided with a SIM card, and an application server in a wireless network using WAP (Wireless Application Protocol) for the data transfer, wherein said SIM card contains a secret/private key, an algorithm for signing of data, a SAT application for handling the signing dialogue and the signing of data.

Description of the Prior Art

Several protocols for data transfer over wireless networks have been proposed by different mobile phone manufactures. Ericsson, Motorola, Nokia Mobile Phones, and Uniwired Planet have developed a joint standard called Wireless Application Protocol (WAP). The purpose of the Wireless Application Protocol is to provide operators, infrastructure and terminal manufactures, and content developers a common environment enabling development of advanced services for digital mobile phones and other wireless terminals or portable communication devices. For example, the WAP enables e-mail and Internet access from a digital mobile phone.

Certain services and WAP applications provided via Internet, such as ordering, order confirmations, bank services, etc, and associated transactions require a high level of security.

WO 99/01848 discloses a procedure, which is applicable for the control of keys to applications making use of the subscriber identity module (SIM) in a mobile phone and for the control of license agreements concerning the use of such applications. Further, the procedure provides data security that allows safeguarding of the interests of the operator, module manufacturer, application developers and users of applications. A key list comprising one or more application-specific keys is stored in the subscriber identity module. A corresponding list is also stored in an application control server connected to the network, which takes care of the control of applications stored in subscriber identity modules. The application stored in the subscriber identity module is activated and/or closed by using the key list.

DE-A1-198 16 575 describes a method for running special applications, such as a virtual charge card, entirely or partly, in a SIM. Further, it is suggested using the SIM toolkit as a means for communication. Security is provided by means of the conventional security means and procedure of the SIM-card. For example, an anti theft security for the special application authorisation and the service data in combination with one or more PIN-codes of the SIM-card.

WO 98/37663 discloses a method for checking authorisation incorporating a way to impart to a smart card an encryption key and including a way to cause a microprocessor, by means of the encryption key and at least one number, to perform a calculation whose result comprises a first signature. The signature together with said number are transferred to a system for which authorisation is to be shown which includes a computer in which said encryption key is stored. The computer is programmed to carry out the calculation to obtain the signature and then to compare the latter signature with the first signature for the verification.

In the above mentioned methods all information transfer is done through SAT (SIM Application Toolkit) applications, in which the security solution also is implemented.

Another way of solving the security problem is to provide one-time password pads, wherein a "new" password is entered via the key pad of the mobile phone or the communication device every time an application is used.

There are several problems and disadvantages associated with the above mentioned prior art solutions. The security level is to low for higher values: passwords could be discovered and the password has to be entered manually making WAP applications very user unfriendly compared to for example pure SAT applications and, of course, the password has to be remembered.

Summary of the Invention

It is an object of the present invention to provide an improved method and system for executing secure data transfer between a communication device, provided with a smart card, such as a SIM card, and an application server in a wireless network using a data transfer protocol such as WAP (Wireless Application Protocol) for the data transfer.

This is accomplished by a method and system according to the invention for executing secure data transfer on the application level for communication applications executing on mobile phones according to the invention. The smart card contains a secret/private key, an algorithm for signing of data, a signing application for handling the signing dialogue and the signing of data. A communiction application, such as a WAP application, is installed on the communication device enabling communication with the application server by means of a dialogue, and information browsing on the server is initiated from the communication device, wherein data are transferred between the server and the

communication device. Further, a request requiring a secure transaction of data is send from the communication device to the server, and an agreement proposal for the secure transaction is send from the server to the communi-cation device. If the agreement proposal is considered acceptable, the agreement proposal is returned to a security adapter. The WAP application in the communication device is suspended or terminated. Details of the transaction to be secured and a sign request are entered into at least a message, such as SMS or USSD packets, from the adapter to the smart card in the communication device in order to activate the signing application. The details of the transaction and a prompt for an accept are displayed on the communication device. If the transaction is accepted, the signing application signs the data to be send with the secret/ private key by using the algorithm, the signed data are send from the communication device to the security adapter via messages. The signature is verified and the verified signed data are send to the server for the final execution of the transaction.

Another object of the invention is to provide an apparatus for connection to a wireless network for monitoring the data transfer between the communication device and the application server.

This is accomplished by a security adapter according to the invention, providing a high level of security in data transfer on the application level for communication applications executing on communication devices.

An advantage of the present invention is that a high level of security in the data transfer is achieved in combination with conventional WAP browsing. An additional advantage is that the application on the SIM card can be made very thin and flexible, because it only has to handle signing of data and no information or menu handling. Further, the system handling the information browsing and

the system handling the security of the transacrtions are separated and, therefore, they can be uppdated and changed independently.

Brief Description of the Drawings

Other objects, advantages and features of the invention will become more apparent from the following detailed description when taken in conjunction with the accompanying drawings, in which

FIG 1 illustrates a first embodiment of a network configuration comprising a security adapter according to the invention,

FIG 2 illustrates a second embodiment of a network configuration comprising a security adapter according to the invention,

FIG 3 is a flowchart of a first embodiment of the method according to the invention, and

FIG 4 is a flowchart of a second embodiment of the method according to the invention.

Detailed Description of the Invention

With reference to FIG 1 of the drawing, there is shown a first embodiment of a network configuration for executing secure data transfer between a communication device, such as a mobile phone, and an application server in a wireless network using WAP (Wireless Application Protocol) for the data transfer. The network configuration comprises a WAP (Wireless Application Protocol) mobile phone 1 - provided with a subscriber identity module (SIM) - for communication with a GSM (Global System for Mobile communications) mobile communication network 2. Additionally, the SIM card contains a secret/private key, an algorithm for signing of data to be transferred, and a SAT (SIM Application Toolkit) application for handling the signing dialogue and the signing of data. The GSM network 2 is

connected to the Internet 3 via a WAP-gateway 4. Further, an application server 5 providing WAP applications is also connected to the Internet 3. Additionally, a security adapter 6 according to the invention is connected to the WAP-gateway for monitoring the communication between the mobile phone 1 and the application server 5.

A second embodiment of a network configuration comprising a security adapter 6 according to the invention is shown in FIG 2. In this embodiment of the network configuration the security adapter 6 is connected to the application server 5.

FIG 3 is a flowchart of a first embodiment of the method according to the invention for executing secure data transfer between a mobile phone and an application server in a wireless network.

In a first step 301, a WAP application, such as a microbrowse, is installed on the mobile phone 1 enabling communication with the application server 5 by means of a WAP dialogue.

A conventional information browsing session on the server is initiated either by a user (subscriber) from the mobile phone 1 or the application server 5 in step 302, wherein data are transferred to/from the mobile phone 1, over the GSM network 2 interfacing the Internet via the WAP gateway, from/to the application server 5. For example, a user browses to a web site providing information accessible via a WAP dialogue from the mobile WAP phone 1. The site belongs to a bookstore offering a service wherein books can be bought directly from the site. A book is selected by the user from a list of books presented on the site. When the user decides to bye the book he selects "order" from an order menu of the site. This action initiates a sequence of operations.

First a request requiring a secure transaction of data is send from the mobile phone to the application

server 5 or from the application server to the mobile phone 1 in step 303. An agreement proposal for the secure transaction is send from the server 5 to the mobile phone in step 304. If the agreement proposal is considered acceptable by the user in step 305, the agreement proposal is send to the security adapter 6 in step 306, and the WAP application in the communication device is suspended or terminated in step 307.

Details of the transaction to be secured and a sign request are entered into at least one SMS or USSD packet by the security adapter 6 in step 308. The SMS packet(s) is send from the security adapter 6 to the SIM card in the mobile phone in order to activate the SAT application in step 309. The details of the transaction and a prompt for an accept from the user are displayed on the communication device in step 310. If the transaction is accepted in step 311, the SAT application signs the data to be send with the secret/private key by using the algorithm in step 312.

The signed data is send from the communication device 1 to the security adapter 6 via SMS or USSD packets in step 313. The security adapter 6 forwards the signature for verification in an entity, such as a backend system, operatively connected to the server 5 in step 314, and the verified signed data is send to the server for the final execution of the transaction in step 315.

A flowchart of a second embodiment of the method according to the invention is shown in FIG 4. A WAP application is installed on the mobile phone 1 enabling communication with the application server 5 by means of a WAP dialogue in step 401.

Information browsing on the server 5 is initiated from either the application server 5 or the mobile phone 1, wherein data are transferred over the network between the application server 5 and the mobile phone 1 in step 402.

Similar to the first embodiment described above, a request requiring a secure transaction of data is send either from the mobile phone 1 to the application server 5 in step 403, or from the application server 5 to the mobile phone 1. However, in this embodiment of the invention an agreement proposal for the secure transaction is send from the server 5 directly to the security adapter 6 in step 404, and the WAP application in the communication device is suspended or terminated in step 405.

Then, details of the transaction to be secured and a sign request are entered into at least one SMS or USSD packet in step 406, the at least one packet is send from the security adapter 6 to the SIM card in the communication device 1 in order to activate the SAT application in step 407. Further, the details of the transaction are displayed on the mobile phone 1 and it is prompted for an accept from the user in step 408. Thus, if the agreement proposal is considered acceptable and the transaction is accepted in step 409, the SAT application signs the data to be send with the secret/private key by using the algorithm in step 410.

The signed data is send from the mobile phone 1 to the security adapter via SMS or USSD packets in step 411, the signature is verified in an entity operatively connected to the server 5 in step 412, and the verified signed data is send to the server for the final execution of the transaction 413.

It is to be understood that even though numerous features and advantages of the present invention have been set forth above, together with details of the configuration and function of the invention, the disclosure is illustrative only.

For example, in alternative embodiments of the invention the security application on the SIM can be activated either directly from the mobile phone or from a bluetooth

connection. In theses cases the answer could be stored in an Elementary File on the SIM card for later retrieval. Further, this should be combined with another Elementary File containing the status of the action.

In another embodiment of the invention a more generic solution for handling the dialogue with the user is implemented. A command interpreter implemented on the SIM card is used, allowing more dynamic downloading/updating of commands defining the application that communicates with the user.

In an alternative embodiment of the network configuration any communication device having transmitting /receiving capability, such as a portable computer, can be provided with a smart card for secure data transfer over a wireless network.

In still another embodiment of the invention the mobile phone have means whereby the user can be assured that he is really communicating directly with the security application and not with an application impersonating the real application. This is implemented as a particular icon, character, font, colour etc only available to certain applications or the operating system in the phone.

In one embodiment of the security adapter 6, it is an electronic apparatus with digital computer capabilities and an internal memory for storage of a computer program product or element. The computer program product comprises software code portions for performing the operation and functions of the security adapter 6, i.e receive an agreement proposal for a secure transaction from the communication device 1, create and send a message to the communication device in order to activate the signing application, receive signed data send from the communication device 1, and send the signed data for verification and then further to the application server 5 for execution of the transac-

tion. In an alternative embodiment, the computer program element is embodied on a computer readable medium.

CLAIMS

1. A method for executing secure data transfer between a communication device (1) and an application server (5), wherein data are transferred over a network (2,3) between the application server (5) and the communication device (1) (301,302;401,402),

characterised by

sending an agreement proposal for a secure transaction of data from the server (5) to a security adapter (6) connected to the network (2,3) (303,304,305,306;403,404),

creating and sending a message from the security adapter (6) to the communication device (1) in order to activate a signing application (307,308,309,310;405,406,407,408),

the signing application signing the data to be send (311,312;409,410),

sending the signed data from the communication device (1) to the security adapter (6) (313;411),

verifying the signature (314;412) for the data, and

sending the verified signed data to the server for execution of the transaction (315;413).

2. A method according to claim 1, **characterised** in that information browsing on the server (5) is initiated from either the application server (5) or the communication device (1), wherein data are transferred over the network (2,3) between the application server (5) and the communication device (1) (301,302;401,402).

3. A method according to claim 1 or 2, **characterised** by, before the step of sending an agreement proposal, the further step of:

sending a request requiring a secure transaction of data, either from the communication device (1) to the application server (5) (303;403), or from the application server (5) to the communication device (1).

4. A method according to any of the preceding claims, **characterised** in that the step of sending a message from the security adapter (6) to the communication device (1) in order to activate a signing application further comprises the steps of:

entering details of the transaction to be secured and a sign request into at least one message (308;406),

sending the at least one message from the security adapter (6) to a smart card in the communication device (1) for activating the signing application (309;407),

displaying the details of the transaction and a prompt for an accept on the communication device (1) (310;408).

5. A method according to any of the preceding claims, **characterised** in that the step of signing the data further comprises the step of:

accepting the transaction (311;409), the signing application signing the data to be send with a secret/private key by using an algorithm (312,410).

6. A method according to any of the preceding claims, **characterised** in that the step of sending an agreement proposal comprises the further step of:

sending the agreement proposal for the secure transaction from the server (5) to the communication device (1) (304) for acceptance (305) before the agreement proposal is send to the security adapter (6) (306).

7. A method according to any of the claims 4-6, **characterised** in that the smart card is a SIM card (subscriber identity module), the data transfer protocol is the WAP (Wireless Application Protocol), the signing application is a SAT (SIM Application Toolkit) application, the communica-

tion application is a WAP application, and the message is at least an SMS or USSD packet.

8. A method according to claim 7, **characterised** in that the WAP application in the communication device is suspended or terminated when the SAT application is activated (307,405).

9. A system for executing secure data transfer between a communication device (1) and an application server (5) over a wireless network (2,3), **characterised** by a security adapter (6) connected to the network (2,3) for monitoring the data transfer between the communication device (1) and the application server (5), wherein

said server (5) is adapted to send an agreement proposal for a secure transaction of data to the security adapter (6),

said security adapter (6) is adapted to receive said agreement proposal for a secure transaction from the server (5), and create and send a message to the communication device (1) for activating a signing application,

said communication device (1) is adapted to sign the data, and send the signed data to the security adapter (6),

said security adapter (6) is adapted to receive, and send the signed data for verification and then send the verified signed data to the application server (5) for execution of the transaction.

10. A system according to claim 9, **characterised** in that said communication device (1) comprises a secret/private key, an algorithm for signing of data, and a signing application for handling a signing dialogue and the signing of data.

11. A system according to claim 10, **characterised** in that said secret/ private key, said algorithm, and said signing application is stored on a smart card such as a SIM card (subscriber identity module), the data transfer protocol is the WAP (Wireless Application Protocol), the signing application is a SAT (SIM Application Toolkit) application, and the message is at least an SMS or USSD packet.

12. A system according to any of the claims 9-11, **characterised** in that said network comprises a mobile telephone network (2) for connection to the communication device (1), the Internet (3) for the connection to the application server (5), and a WAP gateway (4) connecting the mobile telephone network (2) to the Internet (3).

13. A system according to claim 12, **characterised** in that said security adapter (6) is connected to the WAP gateway (4).

14. A system according to any of the claims 9-12, **characterised** in that said security adapter (6) is connected to the application server (5).

15. A system according to any of the claims 9-14, **characterised** in that said communication device is a mobile phone (1) or a portable computer having transmitting /receiving capability.

16. A system according to claim 15, **characterised** in that the mobile phone comprises means for displaying a particular icon, character, font, or colour connected to certain applications or the operating system in the phone, wherein the user can be assured that he is really communicating directly with the security application.

17. A security adapter for connection to a wirless network (2,3) for monitoring the data transfer between a communication device (1) and an application server (5) connected to the network, **characterised** by

means for receiving an agreement proposal for a secure transaction from the communication device (1),

means for creating and sending a message to the communication device (1) in order to activate a signing application,

means for receiving signed data send from the communication device (1), and

means for sending the signed data for verification and then to the application server (5) for execution of the transaction.

18. A computer program product directly loadable into the internal memory of a security adapter (6) with digital computer capabilities, **characterised** by comprising software code portions for performing the steps of:

receiving an agreement proposal for a secure transaction from a communication device (1),

creating and sending a message to the communication device (1) in order to activate a signing application,

receiving signed data send from the communication device (1), and

sending the signed data for verification and then to an application server (5) for execution of the transaction.

19. A computer program element comprising computer program code means to make a security adapter (6) with digital computer capabilities execute the steps of:

receiving an agreement proposal for a secure transaction from a communication device (1),

creating and sending a message to the communication device (1) in order to activate a signing application,

receiving signed data send from the communication device (1), and

sending the signed data for verification and then to an application server (5) for execution of the transaction.

20. A computer program element as claimed in claim 19 embodied on a computer readable medium.

ABSTRACT

A method for executing secure data transfer between a communication device (1) and an application server (5) in a wireless network (2,3), wherein a request requiring a secure transaction of data is send from ether the communication device (1) or the server (5) (303), an agreement proposal for the secure transaction is send to the communication device (1) (304), if the agreement proposal is considered acceptable (305), the agreement proposal is send to a security adapter (6) (306). Details of the transaction are entered into a message (308) and send to a smart card in order to activate a signing application (309) in the smart card. The details of the transaction are displayed on the communication device (310), and if the transaction is accepted (311), the signing application signs the data and send it to the security adapter (6) via messages (313), the signature is verified, and the data is send to the server (315).

To be published with FIG 1

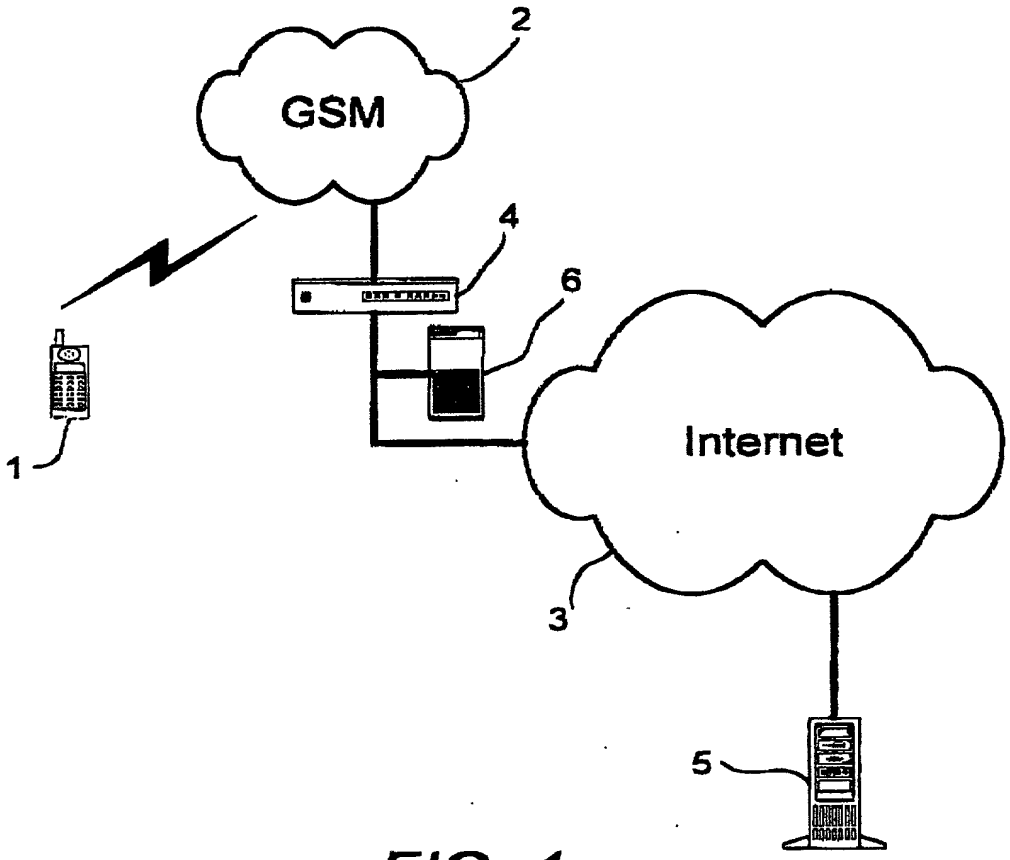

FIG. 1

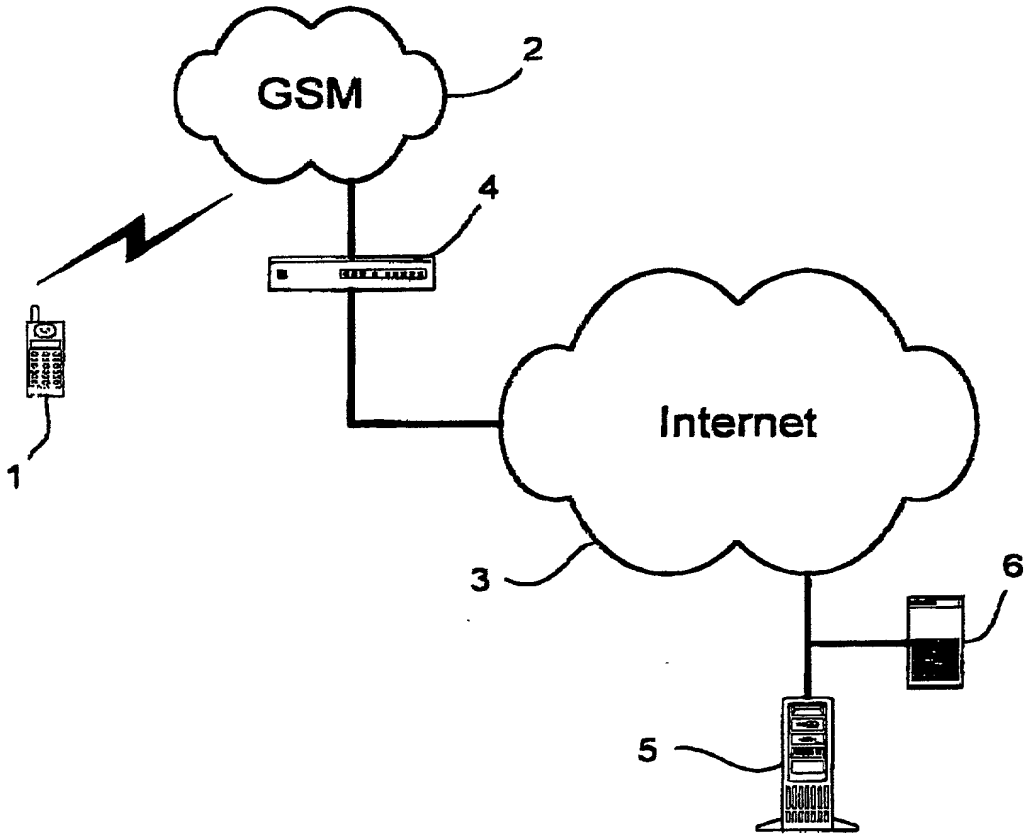

FIG. 2

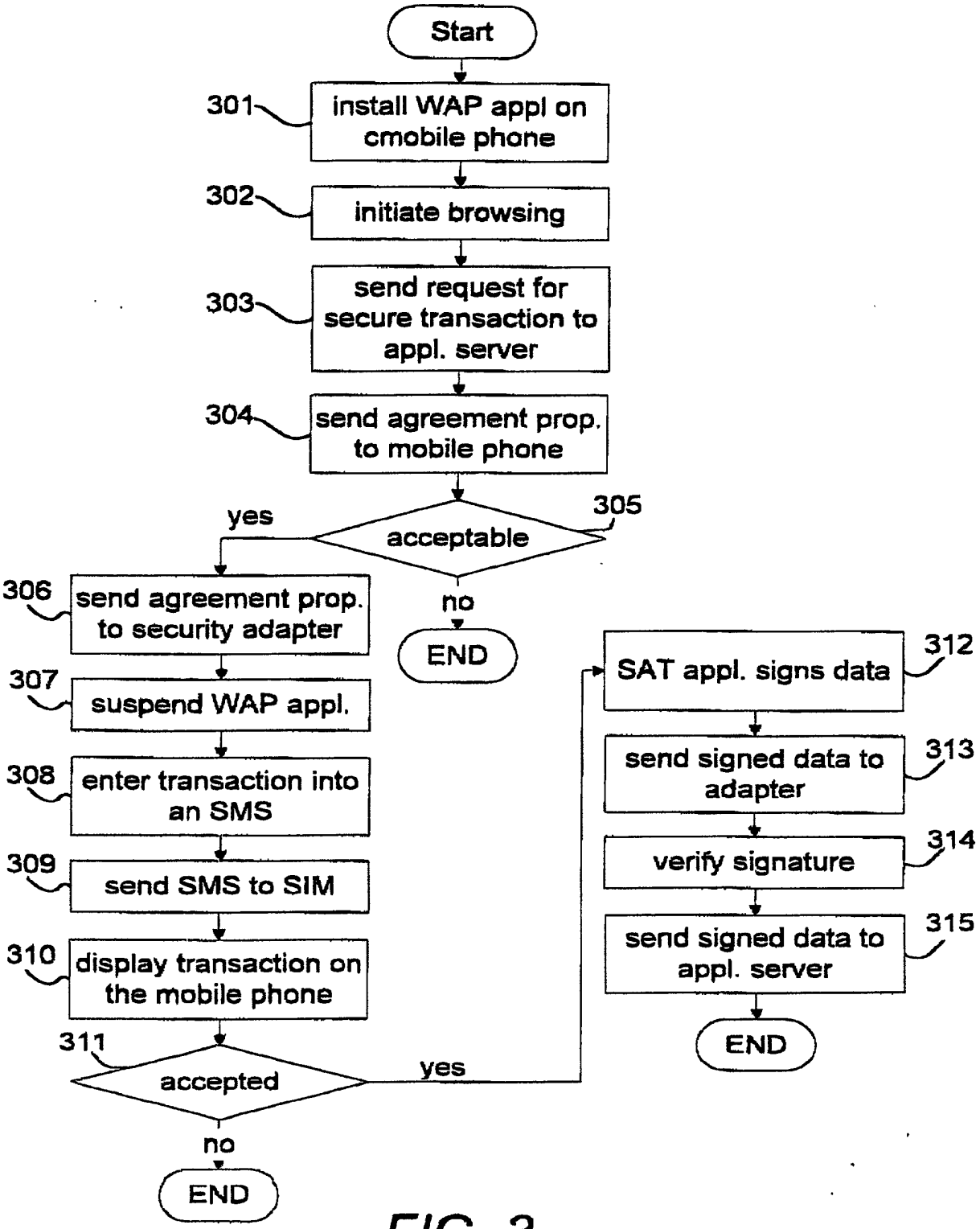
Start
301
install WAP appl on cmobile phone
302
initiate browsing
303
send request for secure transaction to appl. server
304
send agreement prop. to mobile phone
305
acceptable
yes
no
END
306
send agreement prop. to security adapter
307
suspend WAP appl.
308
enter transaction into an SMS
309
send SMS to SIM
310
display transaction on the mobile phone
311
accepted
yes
no
END
312
SAT appl. signs data
313
send signed data to adapter
314
verify signature
315
send signed data to appl. server
END

FIG. 3

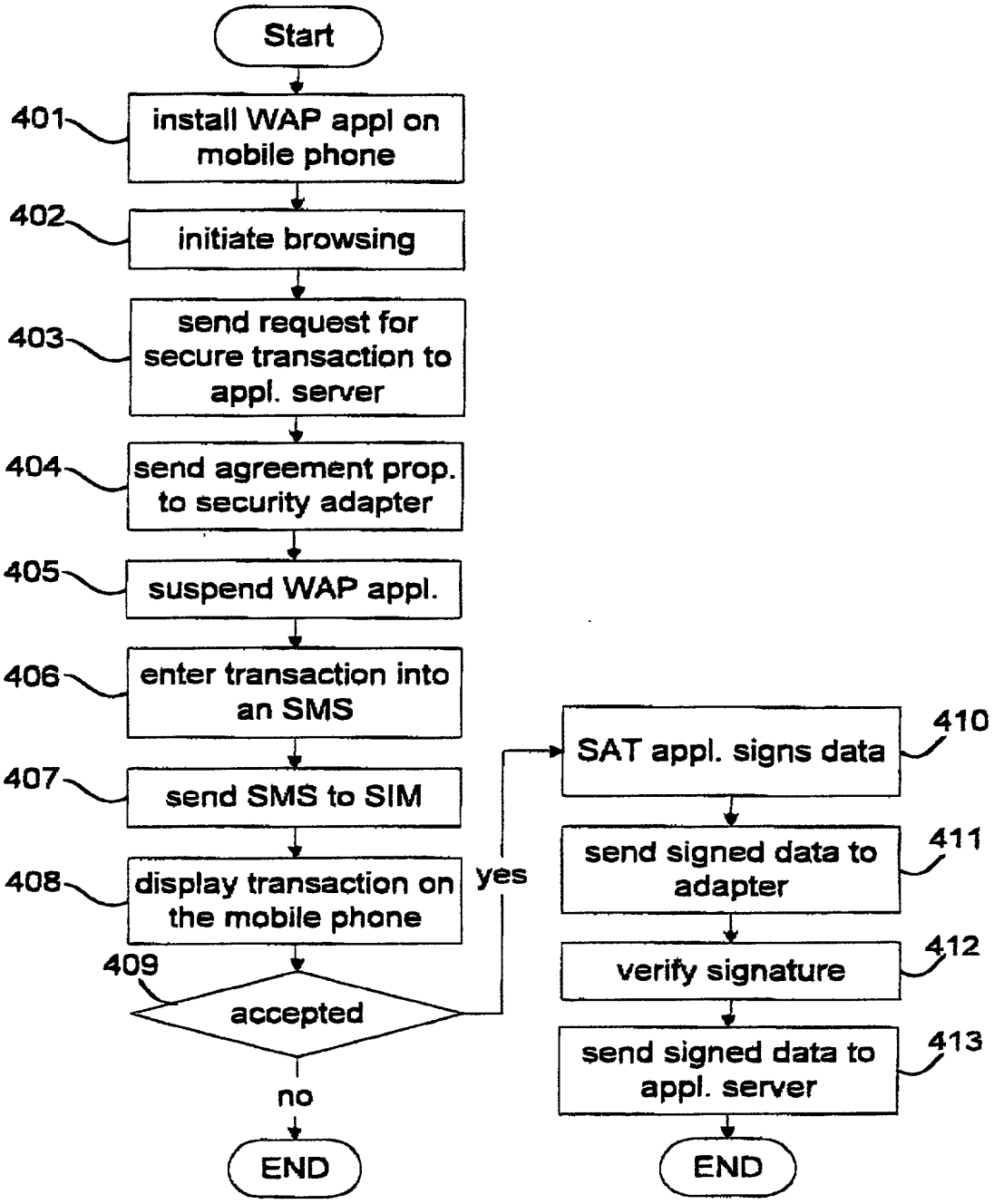
Start
401
install WAP appl on mobile phone
402
initiate browsing
403
send request for secure transaction to appl. server
404
send agreement prop. to security adapter
405
suspend WAP appl.
406
enter transaction into an SMS
407
send SMS to SIM
408
display transaction on the mobile phone
409
accepted
yes
no
END
410
SAT appl. signs data
411
send signed data to adapter
412
verify signature
413
send signed data to appl. server
END

FIG. 4

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (Includes Reference to Provisional and PCT International Applications)	ATTORNEY'S DOCKET NUMBER 026125-069

As a below named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below next to my name;
I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Method and Apparatus for Executing Secure Data Transfer in a Wireless Network

the specification of which (check only one item below):

☒ is attached hereto.

☐ was filed as United States application

Number _____

on _____

and was amended

on _____ (if applicable).

☐ was filed as PCT international application

Number _____

on _____

and was amended under PCT Article 19 and/or PCT Article 34

on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(e) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119:

COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. § 119
Sweden	9903560-2	1 October 1999	X Yes __ No
			__ Yes __ No
			__ Yes __ No
			__ Yes __ No
			__ Yes __ No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

_____ _____
(Application Number) (Filing Date)

_____ _____
(Application Number) (Filing Date)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONTINUED)
(Includes Reference to Provisional and PCT International Applications)

ATTORNEY'S DOCKET NO
026125-069

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States applications(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations § 1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. § 120:

U.S. APPLICATIONS		STATUS *(check one)*		
U.S. APPLICATION NUMBER	U.S. FILING DATE	PATENTED	PENDING	ABANDONED

PCT APPLICATIONS DESIGNATING THE U.S.

PCT APPLICATION NO.	PCT FILING DATE	U.S. APPLICATION NUMBERS ASSIGNED (if any)			

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	Eric H. Weisblatt	30,505	Bruce T. Wieder	33,815
Robert S. Swecker	19,885	James W. Peterson	26,057	Todd R. Walters	34,040
Platon N. Mandros	22,124	Teresa Stanek Rea	30,427	Ronni S. Jillions	31,979
Benton S. Duffett, Jr.	22,030	Robert E. Krebs	25,885	Harold R. Brown III	36,341
Norman H. Stepno	22,716	William C. Rowland	30,888	Allen R. Baum	36,086
Ronald L. Grudziecki	24,970	T. Gene Dillahunty	25,423	Steven M. duBois	35,023
Frederick G. Michaud, Jr.	26,003	Patrick C. Keane	32,858	Brian P. O'Shaughnessy	32,747
Alan E. Kopecki	25,813	Bruce J. Boggs, Jr.	32,344	Kenneth B. Leffler	36,075
Regis E. Slutter	26,999	William H. Benz	25,952	Fred W. Hathaway	32,236
Samuel C. Miller, III	27,360	Peter K. Skiff	31,917		
Robert G. Mukai	28,531	Richard J. McGrath	29,195		
George A. Hovanec, Jr.	28,223	Matthew L. Schneider	32,814		
James A. LaBarre	28,632	Michael G. Savage	32,596		
E. Joseph Gess	28,510	Gerald F. Swiss	30,113		
R. Danny Huntington	27,903	Charles F. Wieland III	33,096		

21839

and: Stephen J. Tytran, Reg. No. 45,846 and Jed W. Caven, Reg. No. 40,551

Address all correspondence to:

21839

Ronald L. Grudziecki, Esquire
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

Address all telephone calls to: Michael G. Savage, Reg. No. 32,596 at (919) 941-9240.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

(7/99)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONTINUED)
(Includes Reference to Provisional and PCT International Applications)

ATTORNEY'S DOCKET NO
026125-069

FULL NAME OF SOLE OR FIRST INVENTOR	SIGNATURE	DATE
Johan KIESSLING		
RESIDENCE	CITIZENSHIP	
Stockholm, SWEDEN	SWEDISH	
POST OFFICE ADDRESS		
Rödabergsbrinken 16, S-113 30 Stockholm SWEDEN		
FULL NAME OF SECOND JOINT INVENTOR, IF ANY	SIGNATURE	DATE
Jan ARWALD		
RESIDENCE	CITIZENSHIP	
Stockholm, SWEDEN	SWEDISH	
POST OFFICE ADDRESS		
Drevkarlstigen 1, S-192 53 Stockholm, SWEDEN		
FULL NAME OF THIRD JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF NINTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		